ORIGINAL

Warren Woodward
55 Ross Circle
Sedona, Arizona 86336
928 204 6434

July 3, 2014

Arizona Corporation Commission (ACC)
Docket Control Center
1200 West Washington Street
Phoenix, Arizona 85007

Re: Docket # RU-00000A-14-0014

Ladies and Gentlemen;

The proposed rules "pertaining to the handling of private customer information" gathered by so-called "smart" meters are lipstick on a pig.

People who do not "opt in" to have their data shared will still be under the same warrant-less "smart" meter surveillance as those who do "opt in".

When are you going to wake up to reality? "Rules" do not protect people's privacy. And once information leaves someone it is no longer private – rules or no rules. At best it may be *confidential* but it is no longer *private*.

It is a fact that "smart" meters are surveillance devices, gathering an unprecedented amount of personal data, data of a type that used to require a warrant. The "smart" grid industry sponsored SmartGridNews recently wrote an article entitled ***Now utilities can tell customers how much energy each appliance uses (just from the smart meter data)***. The article celebrates "smart" meters' ability to report what appliances and other electronic devices people use and when they use them.

The Congressional Research Service's 45 page report, ***CRS Report for Congress, Prepared for Members and Committees of Congress, Smart Meter Data: Privacy and Cybersecurity*** outlines in depth the surveillance capabilities of "smart" meters and the security problems inherent in the "smart" grid.

I have sent hard copies of both documents to you in the past. When will you read and comprehend them?

The CRS report is clear about the impossibility of safeguarding personal "smart"

meter data. From the report: "Even privacy safeguards, such as "anonymizing" data so that it does not reflect identity, are not foolproof. By comparing anonymous data with information available in the public domain, it is sometimes possible to identify an individual—or, in the context of smart meter data, a particular household."

Moreover, the Congressional Research Service warns, "... consumer data moving through a smart grid becomes stored in many locations both within the grid and within the physical world. Thus, because it is widely dispersed, it becomes more vulnerable to interception by unauthorized parties and to accidental breach. The movement of data also increases the potential for it to be stolen by unauthorized third parties while it is in transit, particularly when it travels over a wireless network ...."

Ratepayers therefore should not be lulled into thinking their "smart" meter collected personal data is somehow safe because of some "rules" written by the ACC staff. Hacking is rampant. As investigative reporter Jon Rappoport asks:

> ***Remember Jonathan James, who at the age of 16 put a back-door into DOD's Defense Threat Reduction Agency's server, and stole software from NASA computers that set temperature and humidity at the International Space Station?***
>
> ***Recall Adrian Lamo, who hacked into security systems at B of A, Citigroup, and Cingular?***
>
> ***Keven Poulsen, who hacked into federal computers that record wiretaps?***
>
> ***Tsuromu Shimura, who used a simple cell phone to to hack into phone calls all over Capitol Hill?***
>
> ***The 18-year-old Greek boy, "n-splitter," who was arrested for hacking into systems at Interpol, the Pentagon, the FBI, and the NSA?***
>
> ***I won't even bother mentioning hackers who are hired by the NSA and other agencies.***

And, although I could, I won't bother listing even more hacking reports, including ones that actually happened to me.

At the ACC's March 23, 2012 "smart" meter workshop meeting, APS admitted that they do not have the source codes for their "smart" meters. So APS cannot say with certainty what data is being gathered or who has access to it. Have "backdoors" been built into their "smart" meters? APS does not know and neither do we.

With all of the foregoing in mind, it is clear that people who do not "opt in" to have their data shared will *still* be under the same warrant-less "smart" meter surveillance as those who do "opt in", and they will *still* be vulnerable to third party access to their personal data. The only hope for true, real privacy in the homes of people who do not "opt in" is to get or retain an analog meter.

But, as we all know, in what amounts to extortion, APS is requesting $75 up front and $30 per month for an analog meter.

So, you commissioners will need to decide if, in addition to being complicit in violating people's privacy, you are also going to be complicit in extortion.

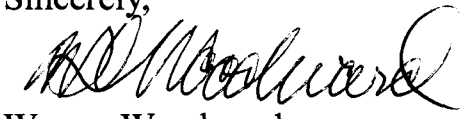
That people are under constant "smart" meter surveillance in their homes whether they opt in or out of data sharing is not made clear in the notice the proposed rules would require utilities to send to ratepayers.

At the very least, all ratepayers should be sent a detailed yet easy to understand explanation of the kind of surveillance they are under – including a graph similar to Figure 1 on page 5 of the CRS report – so they can see just how thorough, intrusive and nonstop "smart" meter surveillance is. Actually, this should have been done before the first "smart" meter was even installed. As I have said repeatedly, there has been no informed consent to the "smart" meter fiasco.

And who is going to make sure a utility tells the truth? For example, for years APS has denied, and continues to deny, the surveillance capabilities of their "smart" meters altogether – and *you* have let them get away with it. Because of your inept, lackadaisical approach to utility regulation and blatant unwillingness to follow state law, I have had to file a formal complaint against APS in an attempt to get them to tell the truth about this and other aspects of their "smart" meters. Under these newly proposed rules will it still be up to citizens to do the work you should be doing?

Will APS be let off the requirement to send out these "opt in" notices since APS denies surveillance altogether?

Sincerely,



Warren Woodward